MULTIMEDIA UNIVERSITY

STUDENT IDENTIFICATION NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

BDS3024 – BUSINESS INTELLIGENCE

(All sections / Groups)

6 MARCH 2017
2.30 p.m. – 4.30 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This question paper consists of 5 pages with 5 questions only.
2. Attempt **ALL** questions. The distribution of the marks for each question is given.
3. Please write all your answers in the Answer Booklet provided.

QUESTION 1

As a general director in your company, the Chief Executive Officer requests you to consider developing the following systems due to the rapid company expansion.

- Human Resource Management System
- Customer Relationship Management System
- Supply Management System
- Enterprise System

Explain the following concepts by using one or all of the above systems:

(a) Portfolio analysis (5 marks)

(b) Risk analysis (5 marks)

(c) Cost-benefit analysis (5 marks)

(d) Balanced scorecard (5 marks)

(Total: 20 marks)

QUESTION 2

(a) Explain the relationship among data warehouse, data mart and databases. (6 marks)

(b) Describe the technical structure of a database. (8 marks)

(c) By using **ONE (1)** example each, explain how dashboard and scorecard can be used to analyse data. (6 marks)

(Total: 20 marks)

QUESTION 3

(a) Explain the differences between Online Transaction Processing (OLTP) and Online Analytical Processing (OLAP). (9 marks)

(b) By using **ONE (1)** example of dummy transaction data, explain how OLTP and OLAP relate to each other. (11 marks)

(Total: 20 marks)

Continued...

QUESTION 4

By using **ONE (1)** diagram, explain clearly how a company can conduct business intelligence by using all of the following sources or platform:

(a) Cloud server

(b) Wifi

(c) Internet

(d) Smartphone

(e) SAP Lumira App

(f) Database

(g) Internet-based

(h) Desktop-based

(i) Thin client

(j) Desktop computer

(Total: 20 Marks)

QUESTION 5 (CASE STUDY)

Semantic Security

Security is a very difficult problem and risks grow larger every year. Not only do we have cheaper, faster computers (remember Moore's Law). We also have more data, more systems for reporting and querying that data, and easier, faster, and broader communication. We have organizational data in the cloud that is not physically under our control. All of these combine to increase the chances that private or proprietary information is inappropriately divulged (leaked).

Access security is hard enough. How do we know that the person (or program) who signs on as Megan Cho really is Megan Cho? We use passwords, but files of passwords can be stolen. Setting that issue aside, we need to know that Megan Who's permissions are set appropriately. Suppose Megan works in the HR department, so she has access to personal and private data of other employees. We need to design the reporting system so that Megan can access all of the data she needs to do her job, and no more.

Continued...

In addition, the delivery system must be secure. A BI server is an obvious and juicy target for any would-be intruder. Someone can break in and change access permissions. Alternatively, a hacker could pose as someone else to obtain reports. Application servers help the authorized user, resulting in faster access to more information. However, without proper security reporting, servers also ease the intrusion task for unauthorized users.

All of these issues relate to access security. Another dimension to security is equally serious and far more problematic: semantic security. Semantic security concerns the unintended release of protected information through the release of a combination of reports of documents that are independently not protected.

Take an example from class. Suppose I assign a group project, and I post a list of groups and the names of students assigned to each group. Later, after the assignments have been completed and graded, I post a list of grades on the Web site. Because of university privacy policy, I cannot post the grades by student name or identifier; so instead, I post the grades for each group. If you want to get the grades for each student, all you have

to do is combine the list from Lecture 5 with the list from Lecture 10. You might say that the release of grades in this example does no real harm - after all, it is a list of grades from one assignment.

But go back to Megan Cho in HR. Suppose Megan evaluates the employee compensation program. The COO believes salary offers have been inconsistent over time and that they vary too widely by department. Accordingly, the COO authorizes Megan to receive a report that lists *SalaryOfferAmount* and *OfferDate* and a second report that lists *Department* and *AverageSalary.*

Those reports are relevant to her task and seem innocuous (not harmful) enough. Nevertheless, Megan realizes that she could use the information they contain to determine individual salaries - information she does not have and is not authorized to receive. She proceeds as follows.

Continued...

Like all employees, Megan has access to the employee directory on the Web portal. Using the directory, she can obtain a list of employees in each department, and using the facilities of her ever-so-helpful report-authoring system, she combines that list with the department and average-salary report. Now she has a list of the names of employees in a group and the average salary for that group.

Megan's employer likes to welcome new employees to the company. Accordingly, each week the company publishes an article about new employees who have been hired. The article makes pleasant comments about each person and encourages employees to meet and greet them.

Megan, however, has other ideas. Because the report is published on SharePoint, she can obtain an electronic copy of it. It is an Acrobat report, and using Acrobat's handy Search feature, she soon has a list of employees and the week they were hired.

She now examines the report she received for her study, the one that has *SalaryOfferAmount* and the *OfferDate*, and she does some interpretation. During the week of July 21, three offers were extended: one for $35,000, one for $53,000, and one

for $110,000. She also notices from the "New Employees" report that a director of marketing programs, a product test engineer, and a receptionist were hired that same week. It is unlikely that they paid the receptionist $110,000; that sounds more like the director of marketing programs. So, she now "knows" (infers) that person's salary.

Next, going back to the department report and using the employee directory, she sees that the marketing director is in the marketing programs department. There are just three people in that department, and their average salary is $105,000. Doing the arithmetic, she now knows that the average salary for the other two people is $102,500. If she can find the hire week for one of those other two people, she can find out both the second and third person's salaries.

You get the idea. Megan was given just two reports to do her job. Yet, she combined the information in those reports with publicly available information and is able to

Continued...

deduce salaries, for at least some employees. These salaries are much more than she is supposed to know. This is a semantic security problem.

(Source: Using MIS, David Kroenke, 2013, P342-343)

Case Study Questions

(a) In your own words, explain the difference between access security and semantic security. (4 marks)

(b) Why do reporting systems increase the risk of semantic security problems? (4 marks)

(c) What an organization can do to protect itself against accidental losses due to semantic security problems? (4 marks)

(d) What legal responsibility does an organization have to protect itself against semantic security problems? (4 marks)

(e) Suppose semantic security problems are inevitable. Do you see an opportunity for new products from insurance companies? If so, describe such a potential insurance product. If not, explain why not. (4 marks)

(Total: 20 marks)

End of Page